Artikel

Datamining in een veranderende wereld van opsporing en vervolging

Mr. dr. S. Brinkhoff*

1. Inleiding

De wereld van opsporing en vervolging is door de digitalisering van de samenleving aan het veranderen. Steeds meer waardevolle (*open source*) informatie is te vinden op het internet, op *social media* en in allerlei gegevensbestanden van publieke en private organisaties. Zo kan op een Twitteraccount zijn gedeeld dat een verdachte in een moordzaak op de plaats delict is geweest, kan op een blog op internet zichtbaar zijn dat een verdachte van een gewapende overval op zoek was naar een vuurwapen, en staat in de bij de Belastingdienst aanwezige gegevensbestanden een schat aan informatie over de inkomenspositie van burgers die waardevol kan zijn in fraudeonderzoeken. Waar de politie en het Openbaar Ministerie (OM) in het verleden veelal alleen gebruikmaakten van klassieke opsporingsmethoden zoals de observatie en de telefoontap, zijn door deze digitalisering nieuwe methoden van onderzoek, zoals geautomatiseerde data-analyse oftewel datamining, in opkomst. Datamining is een methode waarbij digitale gegevens(bestanden) aan elkaar worden gekoppeld en geautomatiseerd, al dan niet met gebruikmaking van een zogenaamd profiel, wordt bekeken of er verbanden bestaan tussen deze gegevens.[1] Datamining kan op een gegevensbestand worden toegepast, maar kan ook worden ingezet om relevante informatie uit echte *Big Data* zichtbaar te maken. *Big Data* ziet op het fenomeen van de steeds groter en complexer wordende hoeveelheden digitale gegevens(bestanden) die bovendien voortdurend en exponentieel in omvang groeien.[2] Datamining is een belangrijke nieuwe methoden van onderzoek voor de politie, omdat deze het mogelijk maakt om naar aanleiding van een zoekvraag de voor de opsporing relevante informatie uit gegevensbestanden te doen oplichten.

De opkomst van datamining als opsporingsmethode roept evenwel, in relatie met het recht op privacy, op tot nadere bezinning over de vraag hoe en in welke gevallen de politie deze opsporingsmethode daadwerkelijk in mag zetten. Met deze vraag in het achterhoofd bespreek ik in dit artikel bestaande vormen van datamining, ga ik in op het privacy-aspect dat verbonden is aan het toepassen van datamining en bied ik een eerste raamwerk voor de regulering van datamining in de opsporing.

* Mr. dr. S. Brinkhoff is als universitair docent straf(proces)recht verbonden aan de vaksectie Straf(proces)recht en Criminologie van de Radboud Universiteit Nijmegen.

1. Zie in dit verband het in 2016 uitgebrachte rapport van de Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving* (te raadplegen op www.wrr.nl), en A.R. Lodder, N.S. van der Meulen, T.H.A. Wisman, L. Meij & C.M.M. Zwinkels, *Big Data, big consequenses. Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak*, WODC-rapport 2014.
2. R. Sietsma, J. Verbeek & J. van den Herik, *Datamining en opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: strafprocesrecht versus recht op privacy*, Den Haag: Sdu Uitgevers 2002.

doi: 10.5553/TBSenH/229567002017003004006

2. Bestaande vormen van datamining in de opsporing

Datamining wordt in de dagelijkse opsporingspraktijk al enige tijd ingezet.[3] Regelmatig ligt een samenwerkingsverband ten grondslag aan het uitvoeren van de geautomatiseerde data analyse.[4]

iCOV

Een eerste voorbeeld van datamining ten behoeve van de opsporing is de infobox Crimineel en Onverklaarbaar Vermogen (iCOV).[5] iCOV is een samenwerkingsverband tussen de politie, Belastingdienst/Douane, FIOD, CJIB, Financial Intelligence Unit en het OM. iCOV levert zogenoemde 'data-intelligence producten' aan de deelnemende organisaties. Daarnaast richt iCOV zich op het ontwikkelen van risico-indicatoren en patronen om witwassen en fraudeconstructies bloot te kunnen leggen. Overheidsinstanties die deelnemen aan iCOV, waaronder dus de politie, kunnen een aanvraag doen voor iCOV-rapportages. Zo'n rapportage biedt inzicht in het bezit en inkomen van een verdachte of laat zien welke formele relaties de verdachte heeft met andere personen of rechtspersonen. Een iCOV-rapportage kan dus worden gebruikt als sturingsinformatie in een al lopend opsporingsonderzoek en lijkt in potentie ook bewijswaarde te hebben. Het (wettelijk) kader voor iCOV wordt gevormd door het Convenant iCOV en de voor elke deelnemende organisatie geldende wettelijke bepalingen over het verstrekken van gegevens. Voor de politie zijn dit de bepalingen van de Wet Politiegegevens. Hieruit lijkt te kunnen worden afgeleid dat de wettelijke grondslag voor het door de politie *gebruik*maken van de resultaten van iCOV wordt gevormd door artikel 3 Politiewet 2012.

iColumbo

Een ander voorbeeld van geautomatiseerde data-analyse ten behoeve van de opsporing is het gebruik van het systeem iColumbo. Dit systeem wordt door de politie aangewend om geautomatiseerd en aan de hand van bepaalde trefwoorden of profielen geautomatiseerd *Big Data* van het internet te bekijken, dit is *open source* informatie, en geautomatiseerd te analyseren met het oog op de opsporing van strafbare feiten.[6] In dit geheel kijkt het systeem iColumbo niet alleen naar actuele gegevens, maar ook naar informatie uit het verleden.[7] De uitkomst van deze data-analyse wordt door iColumbo geordend en op relevantie weergegeven. Het achterliggende idee van de inzet van dit systeem is dat hierdoor het handmatige speuren op het internet overbodig wordt. Over de wettelijke grondslag van de inzet van het systeem iColumbo en het gebruikmaken van de uitkomst van deze vorm van datamining bestaat nog onduidelijkheid. Bij gebrek aan een expliciete wettelijke voorziening lijkt wederom artikel 3 Politiewet 2012 hiertoe te dienen.[8]

FIU

Een derde concreet voorbeeld van datamining in de opsporing gaat schuil in de werkzaamheden van de Financial Intelligence Unit Nederland (FIU-Nederland).[9] Bedrijven en financiële instellingen zijn op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) verplicht ongebruikelijke financiële transacties te melden aan het meldpunt ongebruikelijke transacties van FIU-Nederland. De ongebruikelijke transacties kunnen, na veredeling van de informatie, verdacht worden verklaard. Zoals blijkt uit het jaaroverzicht van de FIU werden in 2016 417.067 ongebruikelijke transacties gemeld, waarvan er uiteindelijk ruim 53.533 (bijna 13%) verdacht zijn verklaard.[10] Veredeling van een gemelde transactie door de FIU kan door middel van datamining geschieden, zo volgt uit het tweede lid van artikel 14 Wwft. De verdacht verklaarde transacties worden na veredeling doorgeleid naar de politie en kunnen aanleiding geven een opsporingsonderzoek te starten, dwangmiddelen toe te passen en dit type informatie kan ook in de bewijsvoering worden betrokken. Wat opvalt is dat voor deze vorm van datamining weliswaar een expliciete wettelijke grondslag bestaat, maar dat hierin geen begrenzing wordt aangebracht. De eis van het bestaan van een verdenking of een controlerende rol van bijvoorbeeld een officier van justitie is hierin immers niet terug te zien. Dit is opmerkelijk nu deze vorm van datamining aantoonbaar tot gevolg heeft dat op grote schaal de in artikel 8 EVRM beschermde privacy van niet-verdachte burgers wordt geschonden. De jaarcijfers van FIU-Nederland laten immers zien dat 87% van de ongebruikelijke transacties *niet* als verdacht worden aangemerkt, terwijl die gegevens door FIU-Nederland wel in het proces van datamining worden betrokken. Zonder wezenlijke aanleiding worden dus de (financiële) gegevens van veel onschuldige burgers door de overheid bekeken en geanalyseerd.

3. Zie Y. Buruma, 'Opvragen, bewerken en kennisnemen van gegevens voor de opsporing', *DD* 2010-57, en J. Kurpershoek, 'Zeecontainers vol data doorzoeken', *Blauw* maart 2014, p. 22-25, over de samenwerking tussen de Rotterdamse recherche en het Kennis- en Expertisecentrum voor Intelligente Data-analyse (Kecida) van het Nederlands Forensisch Instituut (NFI).
4. Zie in dit verband bijvoorbeeld de brief van de toenmalige minister van Justitie van 13 december 2007 en de daarbij gevoegde bijlage 'Programma versterking aanpak georganiseerde misdaad', *Kamerstukken II* 2007-2008, 29 911, nr. 10.
5. Zie het Convenant iCOV 2013, *Stcrt*. 2013, 24607.
6. Zie de notitie 'Vrijheid en Veiligheid in de digitale samenleving', *Kamerstukken II* 2013-2014, 26 643, nr. 298, en T. Timan & E.J. Koops, 'Sociale media en surveillance: over verschuivende rollen en vervagende grenzen', *Strafblad* 2014, p. 284-290.
7. Zie een artikel van M. Roessingh in Trouw d.d. 2 november 2013 getiteld '*iColumbo kan meer dan hij mag*'.
8. E.J. Koops e.a., *Juridische scan open brononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg: TILT 2012.
9. Zie in dit verband D.R. Doorenbos, *Witwassen en voordeelsontneming*, Deventer: W.E.J. Tjeenk Willink 1997, W. Faber & A.A.A. van Nunen, *Uit onverdachte bron. Evaluatie van de keten ongebruikelijke transacties*, Den Haag: Boom Juridische uitgevers 2004, en C.Ch. Mout, 'Gebruikelijk of ongebruikelijk: een bloemlezing van vragen rond de wet MOT', *Advocatenblad* 1994, p. 968-970.
10. Zie <www.fiu-nederland.nl.

doi: 10.5553/TBSenH/229567002017003004006

3. Datamining in de opsporing en het recht op privacy

Zowel de inzet van iCOV als het gebruikmaken van het systeem iColumbo voor de opsporing van strafbare feiten kent dus geen expliciete wettelijke grondslag in het Wetboek van Strafvordering. De wettelijke regeling voor datamining door FIU-Nederland is beperkt. Specifiek voor iCOV en iColumbo lijkt hierdoor het algemeen taakstellende artikel 3 Politiewet 2012 als wettelijke grondslag te gelden. Uit jurisprudentie op het punt van het hanteren van artikel 3 Politiewet 2012 als wettelijke grondslag voor opsporingsbevoegdheden kan worden afgeleid dat dit artikel op zich legitimatie kan bieden voor niet specifiek in de wet geregelde wijze van opsporing, zoals datamining, zolang daardoor slechts een beperkte inbreuk op grondrechten (waaronder het recht op privacy) van burgers wordt gemaakt. Wordt echter een meer dan beperkte inbreuk gemaakt, dan dient hiervoor een specifieke of adequate wettelijke grondslag te bestaan.[11]

De vraag is nu of bijvoorbeeld door de datamining door middel van iColumbo een meer dan beperkte inbreuk op de privacy plaatsvindt, waardoor een expliciete wettelijke regeling noodzakelijk is. Ter beantwoording van deze vraag is het allereerst van belang om aan te stippen dat het recht op privacy wordt beschermd door artikel 8 EVRM. Artikel 7 en 8 van het Handvest van de Europese Unie bieden een soortgelijke bescherming. Het feit dat deze artikelen het recht op privacy beschermen, betekent niet dat de overheid geen inbreuk mag maken op de privacy. Onder bepaalde voorwaarden mag dat wel. Zo wordt in artikel 8 van het Handvest, dat zich richt op de bescherming van persoonsgegevens, bepaald dat de verwerking van privacygevoelige gegevens rechtmatig is zolang er een wettelijke basis voor bestaat. In het tweede lid van artikel 8 EVRM wordt eveneens een kader geschetst voor het op een rechtmatige wijze inbreuk maken op de privacy van burgers. Op basis van dit tweede lid is een inmenging op het recht op privacy rechtmatig als hier een wettelijke regeling voor bestaat, er een legitiem doel bestaat voor de inbreuk en deze inbreuk noodzakelijk is in een democratische samenleving.[12] Op het moment dat door de inzet van datamining als opsporingsmethode dus daadwerkelijk een inmenging plaatsvindt op het recht op privacy van burgers, betekent dit niet automatisch dat deze methode niet als zodanig kan worden ingezet. Het betekent wel dat deze inmenging moet voldoen aan de voorwaarden zoals uiteengezet in artikel 8 EVRM en artikel 8 van het Handvest.

De vraag dient zich nu aan of en wanneer er sprake is van een meer dan beperkte inmenging op het recht op privacy als de politie gebruikmaakt van datamining als methode voor de opsporing van strafbare feiten. In deze context is relevant dat het Europees Hof voor de Rechten van de Mens (EHRM) heeft overwogen dat privacy een veelomvattend begrip is dat zich moeilijk laat definieren.[13] Helder is wel dat het recht op privacy zich niet beperkt tot enkel de bescherming van het privéleven van een burger zoals dat zich bijvoorbeeld afspeelt in de beslotenheid van iemands woning. Het recht op privacy strekt zich ook uit tot het recht om relaties met andere mensen en de buitenwereld aan te gaan en kan ook zien op activiteiten van professionele of zakelijke aard. Het handelen en actief zijn in een publieke omgeving, zoals het internet, kan volgens het EHRM ook onder het bereik van artikel 8 EVRM vallen.[14] Relevant in het kader van de opsporingsmethode datamining is dat het EHRM heeft overwogen dat publiekelijk bekende informatie, zoals de *open source* informatie die op het internet beschikbaar is, binnen het bereik van het recht op privacy kan vallen. Hier is sprake van op het moment dat deze op het internet beschikbare *open source* informatie systematisch door de overheid wordt verzameld en opgeslagen.[15] Door gebruik te maken van het eerdergenoemde systeem iColumbo lijkt nu net dit te gebeuren. iColumbo maakt het immers mogelijk om geautomatiseerd en aan de hand van bepaalde trefwoorden of profielen geautomatiseerd *Big Data* van het internet te bekijken en geautomatiseerd te analyseren. Ook van belang is dat het EHRM in de context van de inlichtingen- en veiligheidsdiensten heeft overwogen dat het systematisch verzamelen en opslaan van gegevens van bepaalde personen een inbreuk oplevert op de privacy van deze personen, zelfs al zijn deze gegevens op een openbare plaats verzameld en zelfs al hebben ze uitsluitend betrekking op de professionele of publieke activiteiten van deze personen.[16]

Op basis van het bovenstaande is de stelling verdedigbaar dat op het moment dat datamining als opsporingsmethode alleen al wordt ingezet om *open source* informatie te analyseren om concrete informatie te krijgen over geïndividualiseerde (verdachte) burgers, dit al een meer dan beperkte inmenging op het recht op privacy oplevert. Hieruit vloeit voort dat van een dergelijk inmenging zeker sprake is als geautomatiseerde data-analyse wordt toegepast op afgesloten gegevensbestanden. Die

11. HR 19 december 1995, *NJ* 1996, 249 m.nt. Schalken. Zie ook HR 14 januari 1997, *NJ* 1997, 371 m.nt. Schalken, Hof 's-Hertogenbosch 8 december 2006, ECLI:NL:GHSHE:2006:AZ4219. Zie ook Rb. Breda 5 september 2006, ECLI:NL:RBBRE:2006:AY7442, HR 1 juli 2014, *NJ* 2015, 114 (*Stille sms*) en 115 (*IMSI-catcher*) m.nt. Van Kempen.
12. D.J. Harris, M. O'Boyle, E.P. Bates & C.M. Buckley, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights*, Oxford: Oxford University Press 2009.
13. D.J. Harris, M. O'Boyle, E.P. Bates & C.M. Buckley, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights*, Oxford: Oxford University Press 2009.
14. Zie bijvoorbeeld EHRM 16 december 1992, appl.nr. 13710/88 (*Niemietz v. Germany*), EHRM 25 september 2001, appl.nr. 44787/98 (*P.G. and J.H. v. the United Kingdom*).
15. Zie bijvoorbeeld EHRM 4 mei 2000, appl.nr. 28341 (*Rotaru v. Romania*) and EHRM 28 april 2003, appl.nr. 44647/98 (*Peck v. the United Kingdom*).
16. EHRM 28 november 2011, appl.nr. 30194 (*Shimovolos v. Russia*).

doi: 10.5553/TBSenH/22956700201700300406

inmenging vereist op grond van het tweede lid van artikel 8 EVRM een specifieke wettelijke grondslag en moet bovendien toegankelijk en voorzienbaar zijn.[17] In deze context is ook nog relevant dat het EHRM, weliswaar meer in de sfeer van de inlichtingen- en veiligheidsdiensten, heeft geoordeeld dat als het om de inzet van *secret measures of surveillance* gaat, het van belang is om hele specifieke wettelijke regels te hebben.[18] Als voorbeeld van een dergelijke *secret measure* kan worden gedacht aan hetgeen door de Snowden-affaire is onthuld over de *mass surveillance* waaraan de Amerikaanse NSA zich schuldig maakte.[19] Het inzetten van datamining als opsporingsmethode zou als een *secret measures of surveillance* kunnen worden betiteld. Het EHRM overweegt dat met name bij dergelijke methoden specifieke wetgeving noodzakelijk is nu het risico op misbruik op de loer ligt en de techniek zich snel ontwikkelt. De wetgeving dient helder te zijn over de aard, de reikwijdte en de duur van de inzet van dergelijke methoden, de voorwaarden waaronder ze kunnen worden toegepast, de autoriteiten die bevoegd zijn om de methoden toe te passen, uit te voeren en toezicht te houden. Op basis van het bovenstaande kan worden geconcludeerd dat de jurisprudentie van het EHRM noodzaakt tot het creëren van een specifieke wettelijke basis voor het gebruik van datamining als opsporingsmethode. Bij het hanteren van de methode vindt immers vrij gemakkelijk een meer dan beperkte inmenging van de privacy plaats. Deze wettelijke regeling ontbreekt op dit moment in ieder geval voor iCOV en voor de inzet van iColumbo. Voor de datamining door de FIU is er wel een wettelijke grondslag, maar die is beknopt.

4. Raamwerk voor een rechtmatige toepassing van datamining voor de opsporing

Op basis van het voorgaande dient zich vervolgens de vraag aan hoe de wettelijke regeling voor datamining als opsporingsmethode eruit moet zien, ook qua bevoegdheidsstructuur. Hiervoor kan aansluiting worden gezocht bij de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017).[20] De artikelen 48, 49 en 50 van deze wet maken het gefaseerd mogelijk ieder soort telecommunicatie: 1) ongericht te verwerven (binnen te halen); 2) voor te bewerken (bijvoorbeeld door de kenmerken, de aard of de identiteit van de gebruiker van de telecommunicatie vast te stellen); en 3) verder te verwerken (bijvoorbeeld door deze te onderwerpen aan geautomatiseerde data-analyse).

Het verdient sterk de voorkeur deze gefaseerde manier van (het gebruik van de uitkomst van) datamining ook toe te passen als de politie geautomatiseerde data-analyse inzet als opsporingsmethode. Voordeel hiervan is dat na elke fase in dit proces van datamining een nieuw beslismoment wordt ingebouwd. Bij dit beslismoment zou telkens ook kunnen worden bepaald dat een hogere autoriteit toestemming moet geven om een verdere verwerking van de gegevens mogelijk te maken. Nu deze methode zich veelal in de opsporingsfase afspeelt kan bijvoorbeeld worden gedacht aan de informatieofficier van justitie en/of de rechercheofficier van justitie die toestemming moet geven voor een nieuwe fase in het proces van datamining. Los van de aanbeveling van het aanbrengen van fasen in het proces van datamining, verdient het ook de voorkeur om wettelijk te regelen op welke gegevens de geautomatiseerde data-analyse betrekking mag hebben. In de huidige situatie bestaat op dit punt immers totaal geen begrenzing of richtsnoer. De Wiv 2017 geeft in deze context ook waardevolle informatie. Zo wordt in het derde en vierde lid van artikel 19 Wiv 2017 een duidelijke begrenzing aangebracht in het soort gegevens dat door de inlichtingen- en veiligheidsdiensten mag worden verwerkt. Uitgangspunt is dat persoonsgegevens die betrekking hebben op iemands godsdienst, ras, gezondheid en seksuele geaardheid niet worden verwerkt, tenzij dit onvermijdelijk is. Het verdient de voorkeur dat een dergelijke begrenzing ook van toepassing wordt op de inzet van datamining in de opsporing.

5. Slot

In dit artikel heb ik laten zien dat de inzet van datamining als opsporingsmethode een expliciete wettelijke grondslag behoeft, ook al beperkt deze geautomatiseerde data-analyse zich tot een analyse van *open source* informatie zoals deze beschikbaar is op het internet. De huidige wettelijke grondslagen lijken in ieder geval niet op basis van de Europeesrechtelijke jurisprudentie te voldoen. Met een blik op de Wiv 2017 zijn suggesties gedaan voor de wettelijke regeling voor datamining als opsporingsmethode. In dit kader heb ik mij uitgesproken voor een wettelijke regeling waarin 1) het proces van datamining gefaseerd plaatsvindt in die zin dat in fasen een verdere verwerking van gegevens plaatsvindt; en 2) de wetgever zich uitspreekt over het soort gegevens dat in de geautomatiseerde data-analyse mag worden bekeken of waarnaar door middel van een zoekvraag mag worden gezocht.

17. Zie bijvoorbeeld EHRM 24 april 1990, appl.nr. 11801/85 (*Kruslin v. France*).
18. Zie bijvoorbeeld EHRM 1 juli 2008, appl.nr. 58243/00 (*Liberty and Others v. the United Kingdom*).
19. Zie over deze affaire rondom Snowden meerdere artikelen in The New York Times op de website <www.nytimes.com.
20. *Stb*. 2017, 317. De oorsprong van deze nieuwe wetgeving ligt in de uitkomsten van het rapport van de Commissie Dessens over de huidige Wiv. Zie Bijlage bij *Kamerstukken II* 2013-2014, 33820, nr. 1 (Evaluatie Wiv. Naar een nieuwe Balans tussen bevoegdheden en waarborgen).

doi: 10.5553/TBSenH/229567002017003004006